GDPR Countdown:
Targeting a Defensible Position by May 2018

Presentation to Legal.IT

Montreal

March 23, 2018

kpmg.ca

Introductions

With You Today

Sylvia Kingsmill

Partner, Data Protection & Privacy
Forensic Services
Risk Consulting

François Senécal

Manager
Information Management and eDiscovery

Discussion Topics

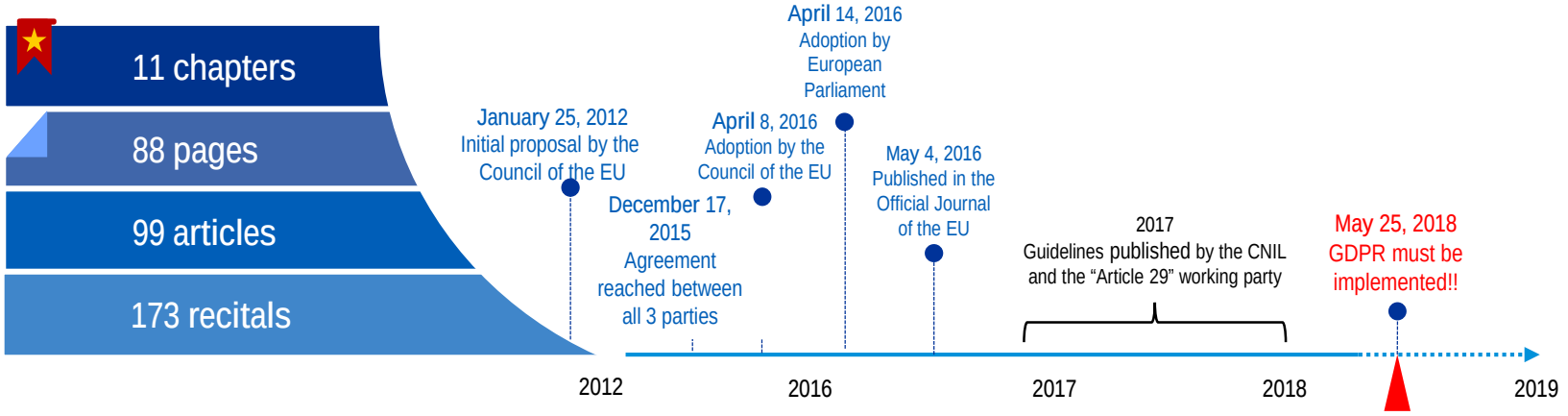
1. GDPR Overview
2. Key GDPR Impacts
3. Market Observations
4. Next Steps
5. Closing Thoughts

KPMG

GDPR Overview

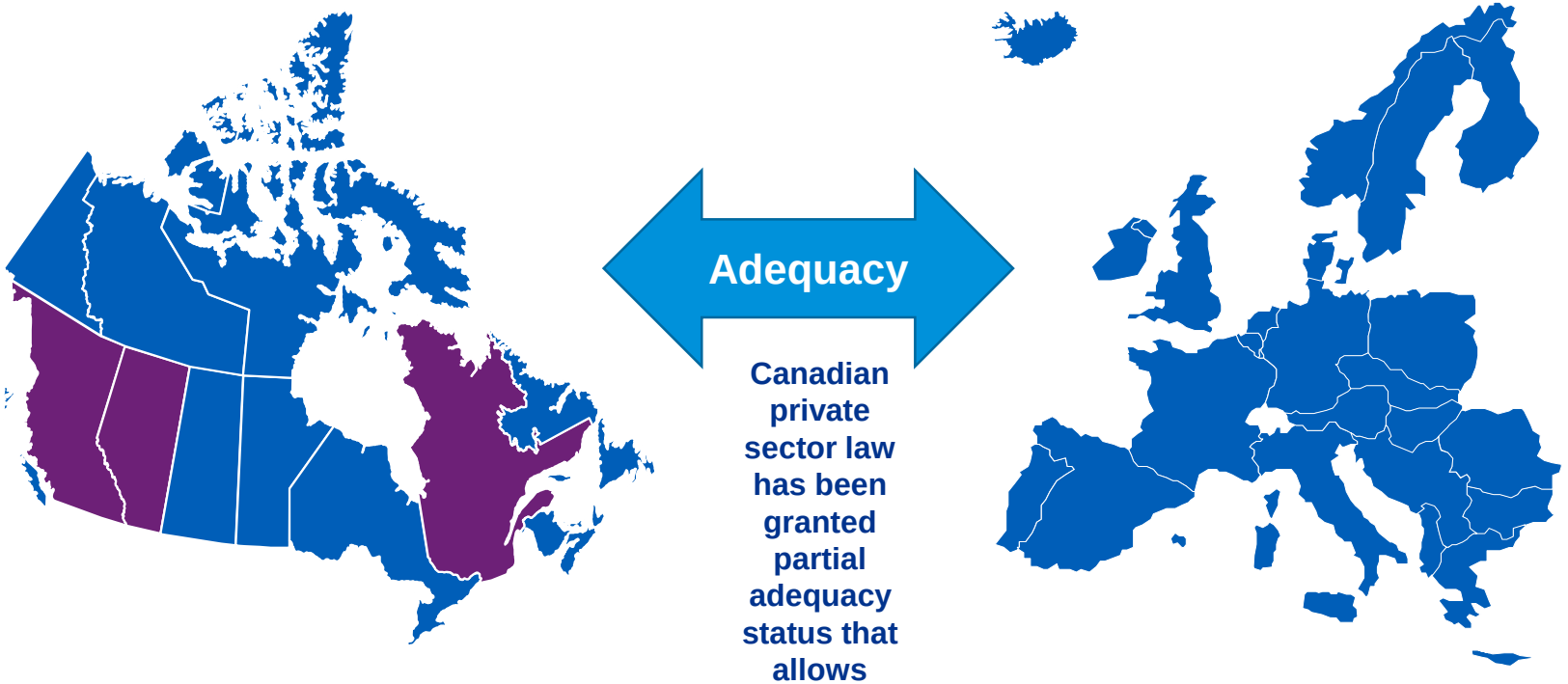
The Wait is Finally Over!

- The EU General Data Protection Regulation (GDPR) will reform, modernize and replace the 1995 EU Data Protection Directive
- The objective is to harmonize data protection rules across 28 EU member states by creating a single, comprehensive EU data protection framework for the processing of and free flow of data, with a one-stop shop mechanism for enforcement
- The reform aims to give control to EU citizens and strengthen consumer trust in digital economy



Where does Canada stand?

Under EU law, one way to transfer personal data abroad is on the basis of an EU Commission "adequacy" decision confirming that the non-EU country provides a level of data protection "***essentially* equivalent**" to that in the EU.



EU's New Privacy Regime "Raises the Bar"

Privacy Commissioner Daniel Therrien says "It creates impetus, if not pressure, on other countries and economies of the world to at least consider whether the GDPR rules should be adopted in their own jurisdictions." *The Globe and Mail, March 4 2018.*

Parliamentary report released on February 28th 2018 identified 19 recommendations to update and modernize the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Key Finding:

PIPEDA is going to change

1. PIPEDA is not fit for purpose
2. Canada is at risk of losing adequacy standing
3. Calling for order-making powers, better consent rules and adoption of privacy by design

Why (s)care?

HUGE FINES

- The GDPR introduces fines of up to €20 million, or 4% of worldwide annual turnover, whichever is higher
- The GDPR allows individuals to seek monetary damages in court

REAL REPUTATIONAL RISK

- Enforcement activities by Data Protection Authorities (DPAs) will increase. Data protection breaches will make the headlines sooner.

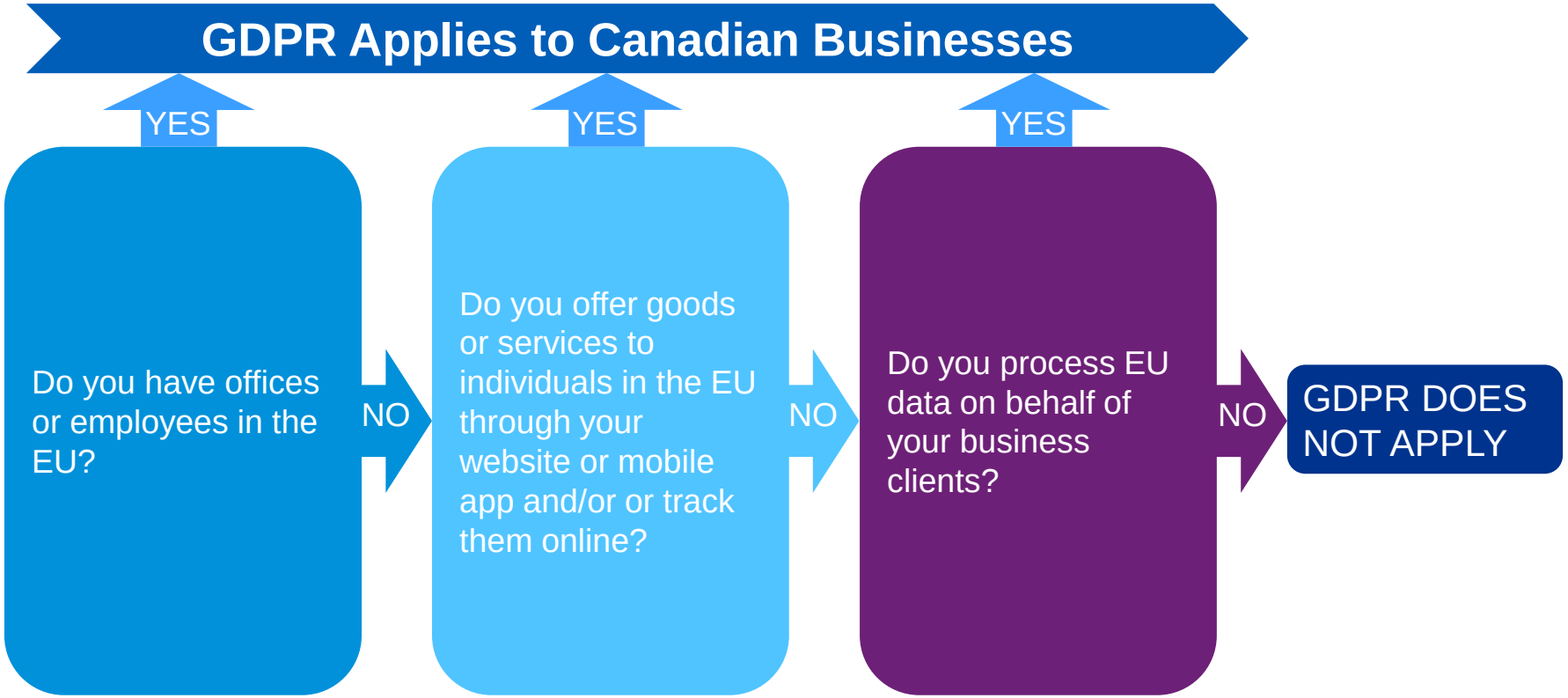
OVERSIGHT/ENFORCEMENT

- Harmonized enforcement actions across EU with “one-stop shop” cooperation
- New Data Protection Board will resolve disputes among DPAs

Objects in mirror are closer than they appear

The GDPR will apply to **ALL organizations established in the EU** that process EU data and **ANY organization that processes data about EU residents or citizens within the EU** that relate to:

- ✓ Offering goods or services; or
- ✓ Monitoring the behaviour of EU residents/citizens.



Key Roles and Responsibilities under the GDPR

Data Subject means an individual who is the subject of personal data. In other words, the data subject is the individual whom the personal data is about.

Data Processor in relation to personal data, means any person who processes the data on behalf of the data controller

Data Controller is a person/organization who (either alone or jointly) determines what, how, why and for what purpose(s) any personal data is processed

Lawful and Fair Processing

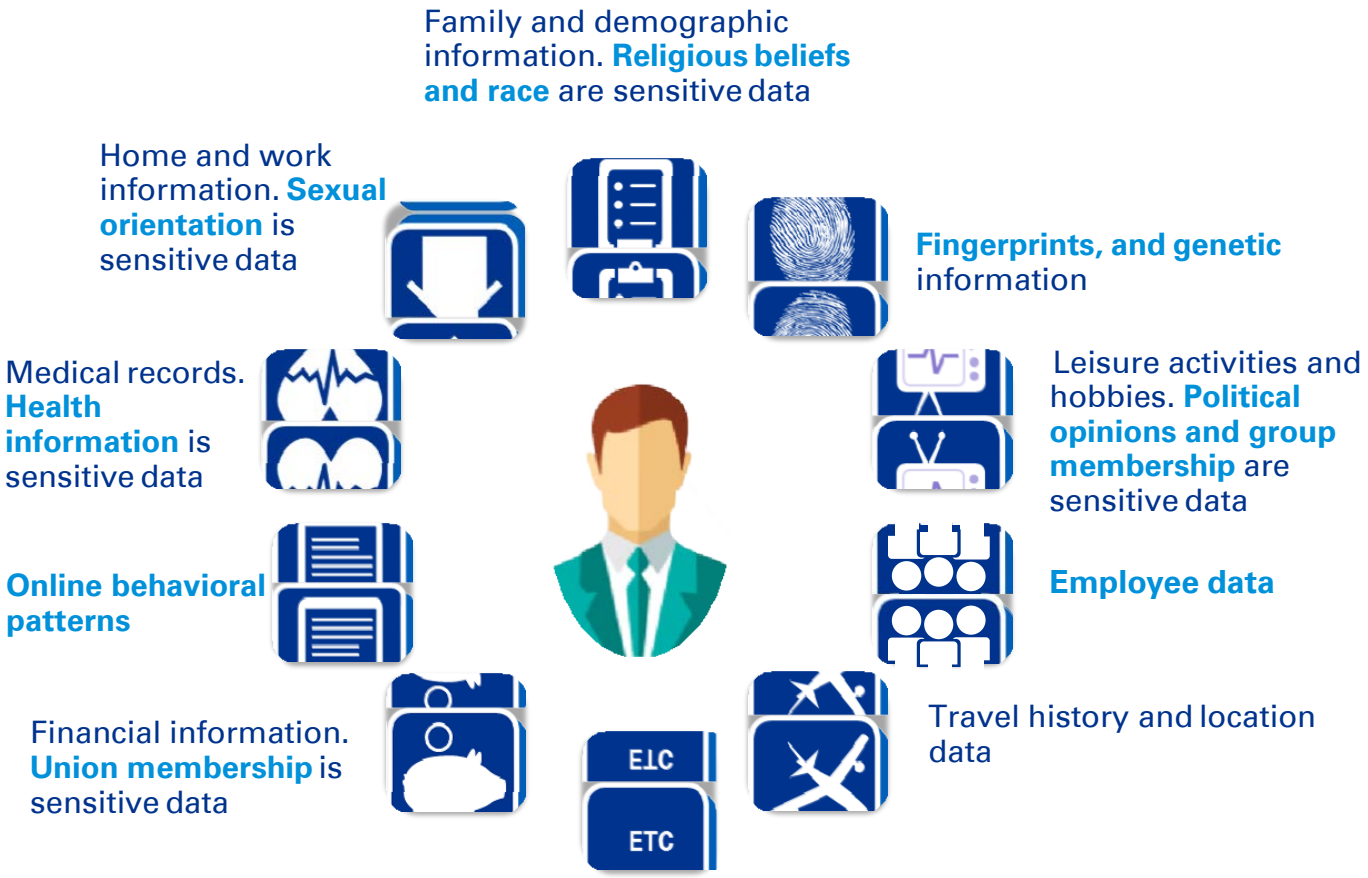
The General Rule:

- ✓ Data Controller must have a legal basis for collecting Personal Data and must protect Personal Data throughout information lifecycle (from acquisition to disposition).
- ✓ Data Processors must provide sufficient guarantees they comply with GDPR and help protect Data Subject rights.

Legal Grounds for Processing

1. Consent
2. Legal obligation
3. Performance of contract
4. Protect the interests of the Data Subject
5. Public Interest or official authority
6. Legitimate interests

What is Personal Data?



KPMG

Key GDPR Impacts

What is Different?

The GDPR has both heightened and new requirements:

Third Party Risk Management

Vendors and suppliers must provide "sufficient guarantees" of appropriate technical and organizational measures, reflected in third-party vendor contracts.

Recordkeeping

Data Controllers will have to identify and inventory processes and systems handling personal information, and must be prepared to demonstrate compliance on demand.

Data Subject Rights

Data Controllers must be prepared to respond to requests for access, correction, deletion, transfers, or any objections to processing, which all depend on the legal basis for processing.

Accountability and Transparency

Heightened expectations for accountability and transparency for Data Controllers and Processors.

Mandatory Data Breach Notification

Data Controllers have 72-hour window by which they need to report breaches to the regulators and to Data Subjects where it is likely to affect their rights and freedoms. Data Processors must also report privacy breaches.

Data Protection by Design & DPIAs

Privacy must be built into design of system architectures and processes from the start!

A DPIA is required for any data processing posing a high risk or for all new data processing technologies being introduced, including profiling and predictions about Data Subjects.

IT Enables : Processes

Data Protection by Design

- Implies a “trilogy” of encompassing applications: IT systems (e.g., secure coding)/accountable business practices (e.g., regular testing of security controls)/physical design and networked infrastructure (e.g., privacy settings by default)

Data Minimization

- Pseudonymization, anonymization, tokenization or other data minimization tools

Record-Keeping/Reporting

- Tracking and recording of data processing, transfer, access, disclosure activities and objection requests (correction, portability and erasure);
- Inventory and catalogue of all GDPR events (remediation, breaches, notifications, processing, consents, remediation)

Legitimation

Consent

- Consent management – track and store consent (meta data) that shows method and purposes of collection) and allows consent to be withdrawn at any time & ensures that processing is stopped

Cross-border Transfers

- Identification, cataloguing, and classification of unstructured data (e.g. data mapping & discovery); tracking of customer data exports/profiling and email archives stored on-premises or in cloud

Individual rights

Data Portability

- Data extraction & export mechanism

Right to Object

- Tracking and recording of data subject rights:
  - Data access, correction, portability and erasure
  - Objection to and restriction of processing
  - Automated individual decision-making, including profiling

Right to be Forgotten

- Data extraction & purge (profile deletion tool) or algorithm in the system (including for back ups)

Information security

Breach Notification

- Get ready to be ready (72h is not that long)
- Audit logging, system monitoring of privileged access (alert triggers) and reporting

Security for Processing

- Encryption, pseudonymization and/or anonymization techniques (obscures the connection of data to an individual)
- Confidentiality, integrity, availability and resilience of processing systems and services in compliance with security standards, including identity and access management, perimeter and end-point security
- Privacy Enhancing Technologies for breach identification (e.g. penetration testing, threat detection, anti-malware, privileged user monitoring
- Data Loss Prevention Tools (DLP)

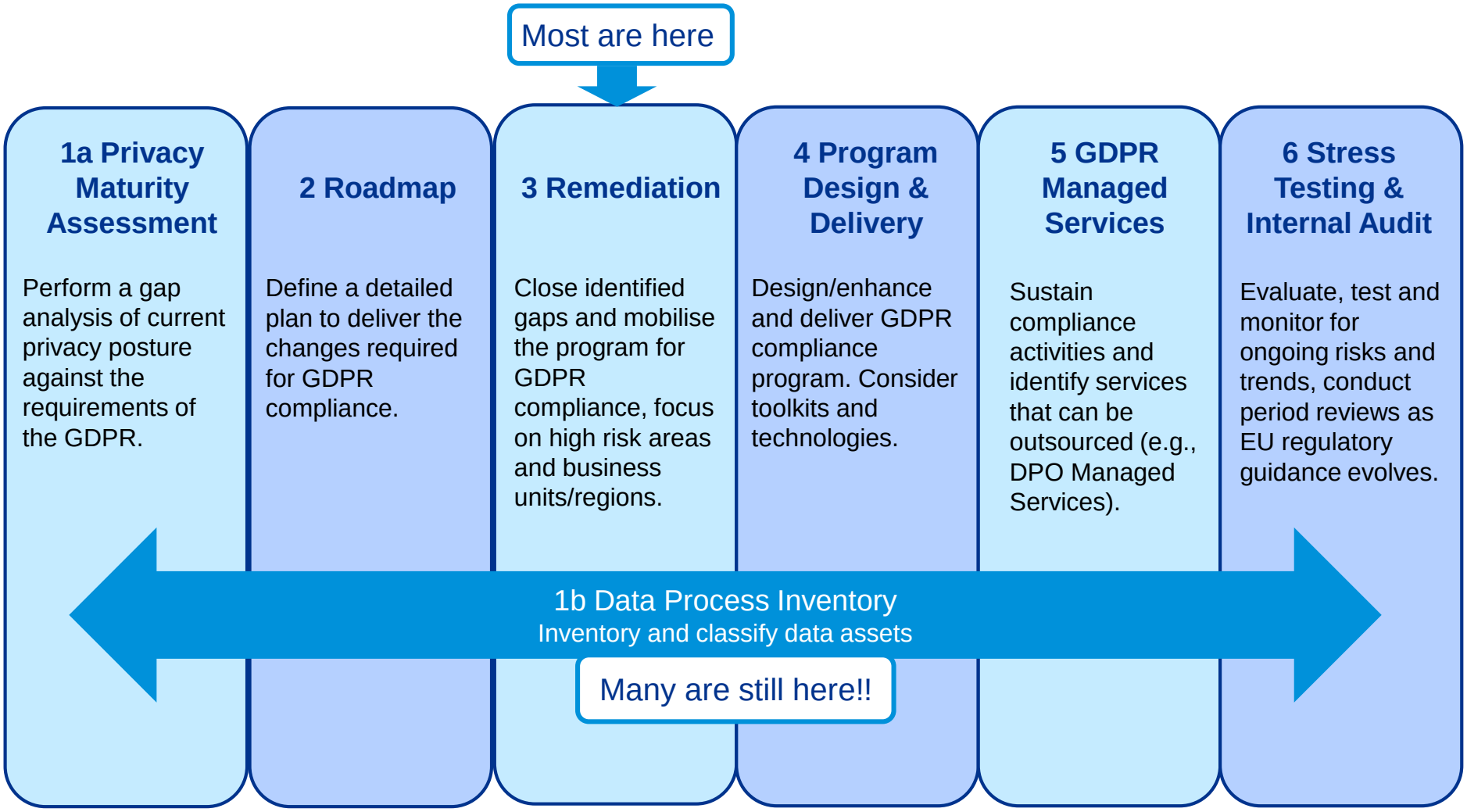
Secure Destruction

- Data redaction/hashing tools
- Review of backup methods

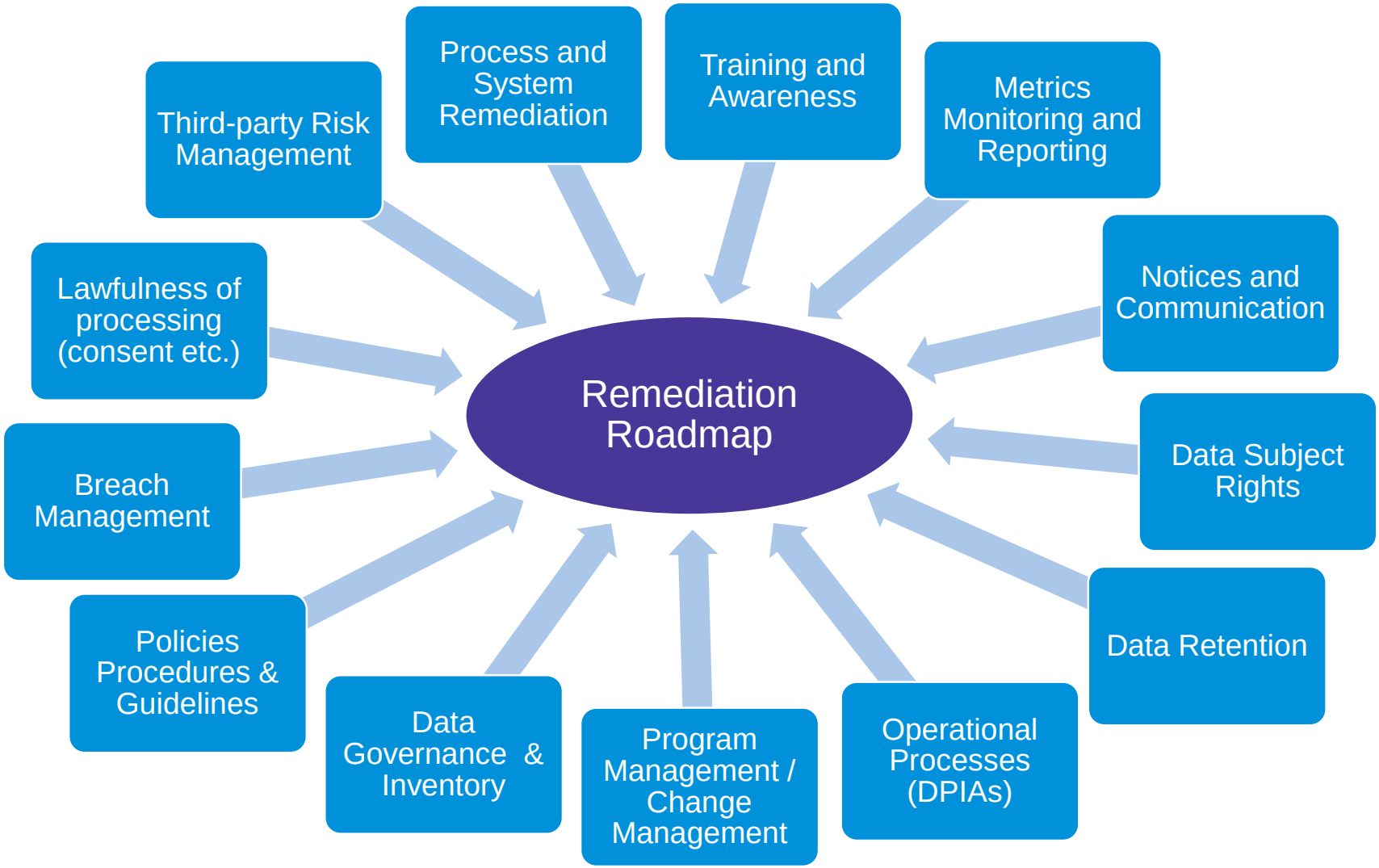
KPMG

Market Observations

Where are You On Your GDPR Journey?



GDPR Work Streams



Key Implementation Challenges

Executive Sponsorship

Senior visibility and sponsorship is key. Tone from the top will drive cultural shift and behaviours for privacy best practices where privacy is treated as a business issue and critical trust factor for the customer experience.

Program Ownership

The **workload** involved in attaining GDPR compliance is often **underestimated**. As a result, it will be necessary to **communicate** and **build awareness** at the outset of the project in order to help prepare the teams and organize for the implementation phase in terms of ownership, budget and ongoing program governance.

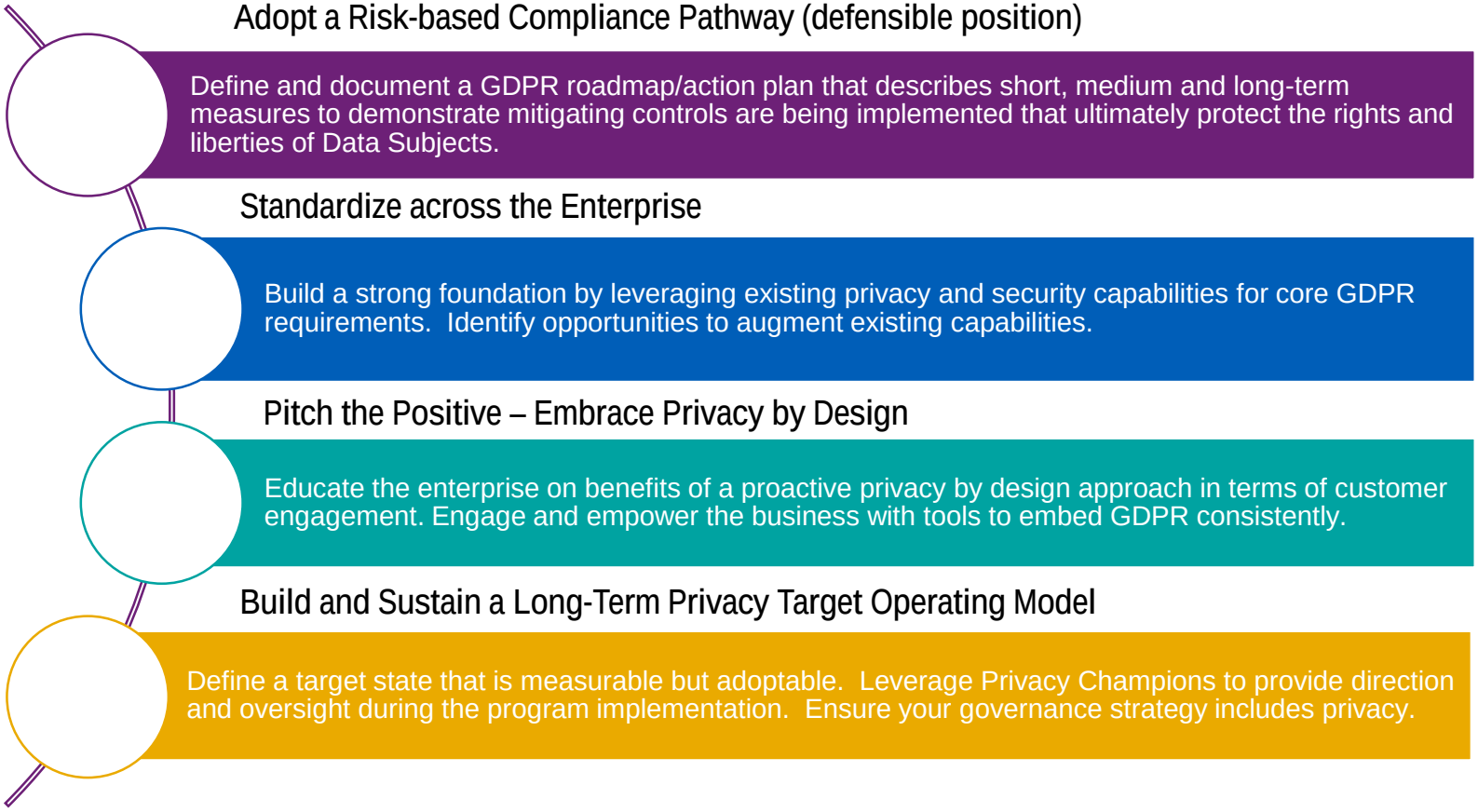
Implementation Approach

GDPR implementation is cross-functional and requires the **contribution** of **many disciplines** (privacy, security, data analytics, IT, business, legal). As a result, **all stakeholders** must be mobilized and brought in at the outset of the project and **their involvement must be ensured** throughout.

Training and Awareness

The GDPR project must have an integral **learning dimension** so that all stakeholders adhere to the principles of the GDPR (such as Accountability), **understand its impact** on current and future activities and **get involved** in the project, such that GDPR compliance is **sustained over the long term**.

Critical Success Factors



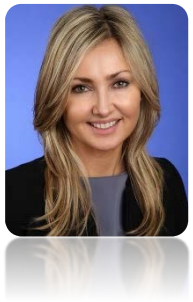
KPMG

Closing Thoughts

Remember:

1. It’s business as usual… don’t panic!
2. Mitigate risk exposure rather than strive for full compliance
3. Think long term – it’s about customer trust

Thank you!



Sylvia Kingsmill

Partner

+1 647-534-1080
skingsmill@kpmg.ca

François Senécal

Manager

514-840-2342
fsenecal@kpmg.ca

kpmg.ca